Workplace Investigations

Contributing Editors

Phil Linnard at Slaughter and May
Clare Fletcher at Slaughter and May

07. What data protection or other regulations apply when gathering physical evidence?

Hong Kong

Author: *Wynne Mok, Jason Cheng, Audrey Li*
at Slaughter and May

If physical evidence contains data relating to an individual, from which the identity of the individual can be ascertained,[1] the data would constitute personal data under the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). The PDPO sets out several data protection principles that the employer must comply with while processing personal data, including:[2]

- personal data must be collected for a lawful purpose related to a function or activity of the employer and should not be excessive for this purpose. An internal investigation would be regarded as a lawful purpose;
- personal data must be accurate and not kept longer than is necessary;
- personal data must not be used for a purpose other than the internal investigation (or other purposes for which the data was collected) unless the employee consents to a new use or the new use falls within one of the exceptions provided in the PDPO;
- personal data must be safeguarded against unauthorised or accidental access, processing or loss; and
- the employee whose personal data has been collected has the right to request access to and correction of his or her personal data retained by the employer.

If an employer wants to gather evidence through employee monitoring, it should ensure that the act of monitoring complies with the data protection principles of the PDPO if the monitoring activity would amount to the collection of personal data. The Privacy Commissioner for Personal Data has issued guidelines to employers on the steps they can take in assessing whether employee monitoring is appropriate for their businesses.[3] As a general rule, employee monitoring should be conducted overtly. Further, those who may be affected should be notified in advance of the purposes the monitoring is intended to serve, the circumstances in which the system will be activated, what personal data (if any) will be collected and how the personal data will be used.

Covert surveillance of employees should not be adopted unless it is justified by relevant special circumstances. Employers should consider whether there is reason to believe that there is an unlawful activity taking place and the use of overt monitoring would likely prejudice the detection or collection of evidence.[4] Even if covert monitoring is justified, it should target only those areas in which an unlawful activity is likely to take place and be implemented for a limited duration of time.

[1] PDPO section 2.

[2] PDPO Schedule 1.

[3] PCPD, “Privacy Guidelines: Monitoring and Personal Data Privacy at Work” (April 2016) <https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/Monitoring_and_Personal_Data_Privacy_At_Work_revis_Eng.pdf>.

[4] Ibid at paragraph 2.3.3.

Last updated on 15/09/2022

Netherlands

Author: *Barbara Kloppert, Mirjam Kerkhof, Roel de Jong*
at De Brauw Blackstone Westbroek

Dutch data protection rules are based on the EU Data Protection Directive. The employer has to notify the Dutch Data Protection Authority when processing personal data as part of an internal investigation. Given that the notification can be accessed publicly, it is recommended that the employer give a sufficiently high-level description of the case. In addition, the description should be sufficiently broad to include the entire investigation, and any future expansions of the scope of the investigation. Often companies make filings for all future internal investigations, without referring to specific matters.

The employer has to notify employees whose personal data is being processed about – among other things – the purposes of the investigation and any other relevant information. According to the Dutch Data Protection Act, this information obligation may only be suspended on restricted grounds, i.e. if the purpose of the investigation is the prevention, detection and prosecution of crimes and postponement is necessary for the interests of the investigation (e.g., because there is a risk of losing evidence, or collusion by individuals coordinating responses before being interviewed)). These exceptions on the duty to inform involved persons must be interpreted very restrictively. As soon as the reason for postponement is no longer applicable (e.g., because the evidence has been secured), the individuals need to be informed.

Dutch data protection law does not require the consent of employees. Consent given by employees, however, also cannot compensate for a lack of legitimate purpose or unnecessary or disproportionate data processing, as the consent given by an employee to its employer is not considered to be voluntary given the inequality of power between them.

Furthermore, internal company policies may contain specific data protection rules.

Last updated on 27/11/2023

Switzerland

Author: *Laura Widmer, Sandra Schaffner*
at Bär & Karrer

The Swiss Federal Act on Data Protection applies to the gathering of evidence, in particular such collection must be lawful, transparent, reasonable and in good faith, and data security must be preserved.[1]

It can be derived from the duty to disclose and hand over benefits received and work produced (article 321b, Swiss Code of Obligations) as they belong to the employer.[2] The employer is, therefore, generally entitled to collect and process data connected with the end product of any work completely by an employee and associated with their business. However, it is prohibited by the Swiss Criminal Code to open

a sealed document or consignment to gain knowledge of its contents without being authorised to do so (article 179 et seq, Swiss Criminal Code). Anyone who disseminates or makes use of information of which he or she has obtained knowledge by opening a sealed document or mailing not intended for him or her may become criminally liable (article 179 paragraph 1, Swiss Criminal Code).

It is advisable to state in internal regulations that the workplace might be searched as part of an internal investigation and in compliance with all applicable data protection rules if this is necessary as part of the investigation.

---

[1] Simona Wantz/Sara Licci, Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, in: Jusletter 18 February 2019, N 52.

[2] Claudia Fritsche, Interne Untersuchungen in der Schweiz, Ein Handbuch für Unternehmen mit besonderem Fokus auf Finanzinstitute, p. 148.

Last updated on 15/09/2022

Contributors

Hong Kong

Wynne Mok
Jason Cheng
Audrey Li
Slaughter and May

Netherlands

Barbara Kloppert
Mirjam Kerkhof
Roel de Jong
De Brauw Blackstone Westbroek

Switzerland

Laura Widmer
Sandra Schaffner
Bär & Karrer